Proceeding of The 6th Annual Basic Science International Conference
Published online, on June 7, 2016.

A Cryptographic Algorithm based on Max plus Wavelet Transform

Joko Cahyono[1*], Subiono[2]

[1]Postgraduate Student of Department of Mathematics, Faculty of Mathematics and Natural Sciences, Sepuluh Nopember Institute of Technology, Surabaya, Indonesia
[2]Department of Mathematics, Faculty of Mathematics and Natural Sciences, Sepuluh Nopember Institute of Technology, Surabaya, Indonesia
* Corresponding authors: [j0k0_cahy0n0@yahoo.com]

Abstract – Cryptography is one of the tools to secure information. In this paper, a cryptographic algorithm based on max plus wavelet transform is constructed. The encryption is done based on analysis process, while the decryption is done based on synthesis process. The key consists of two elements. The first element is the number of the channels used. The second element is the code of the detail signals. The running time analysis shows that this algorithm is fast because it involves only a maximum and addition operation. The encryption and decryption time increase linearly along with increasing length of the text. The correlation analysis shows that almost no linear correlation between the plaintext and cipher text.

1. INTRODUCTION

Cryptography is the science of the encryption technique where data is scrambled using an encryption key to be something that is difficult to be read by someone who does not have the decryption key [5]. Until now many varieties of cryptographic algorithms have been constructed. Goswami et al proposed cryptographic algorithm based on discrete wavelet transform [1]. They used Daubechies wavelet transform. Fahim in his thesis [2] constructed wavelet transform using max plus algebra. The advantage of max plus wavelet transform is not involve floating point, so it becomes simple and efficient for computing.

Max plus algebra and min plus algebra also have been used in cryptography. Grigoriev and Shpilrain [3], Durcheva [4] in their papers discussed the use of max plus algebra and min plus algebra in cryptography. Max plus algebra and min plus algebra are used for key generating.

Based on the description above, in this paper we constructed a cryptographic algorithm based on max plus wavelet transform. We used max plus wavelet transform type A. Max plus wavelet transform is used for encryption, decryption and key generating. Then the feasibility of the proposed algorithm will be tested. The analysis is done using the running time and the correlation value between plaintext and cipher text.

2. METHODS

2.1 Max Plus Wavelet Transform

The wavelet transform is used in signal processing. The analysis operation is done on the main signals that have high resolution to obtain the approximation signal and detail signals. The approximation signal represents the main signals but has a lower resolution. The detail signals ensure that the main signals can be recovered by the synthesis process. The wavelet transform scheme is given in Figure 1.

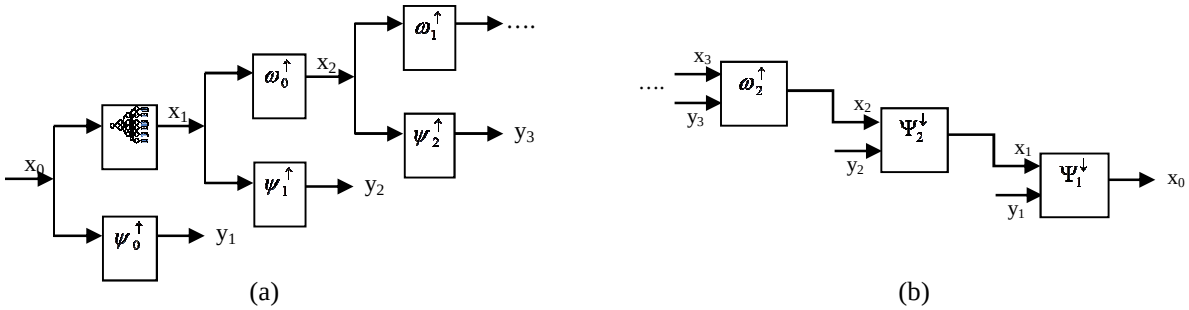

Figure 1 The Wavelet Transform Scheme
(a) Analysis Process (b) Synthesis Process

The wavelet transform is divided into discrete wavelet transform and continuous wavelet transform. The Haar wavelet transform is the simplest discrete wavelet transform. In Haar wavelet transform, the main signals are decomposed into an approximation signal and detail signal series. Approximation signal is obtained by compute the average of the main signals. Based on Haar wavelet transform, Fahim constructed wavelet transform using max plus algebra. Max plus algebra is algebra structure that involves only maximum and addition operation [7]. Fahim constructed five types of max plus wavelet transform.

In type A, there are analysis operations $\psi_j^{\uparrow}$ and $\omega_j^{\uparrow}$, and synthesis operation $\Psi_j^{\downarrow}$. In analysis operation, input are p signals, while output are an aapproximation signal and p-1 detail signals. In synthesis operation, input is an approximation signal and p-1 detail signals, while output are p signals. Scheme of max plus wavelet transform type A is given in Figure 2.

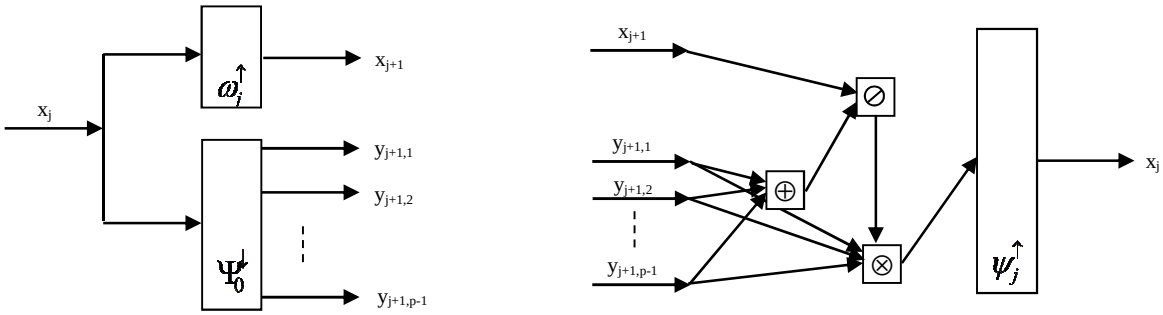

Figure 2 the Scheme of Max Plus Wavelet Transform Type A

(a) Analysis Process (b) Synthesis Process

Based on Figure 2, analysis operation are constructed as follows:

$$\psi_j^{\uparrow}(x_j)[n] = \bigoplus_{k=0}^{p-1} x_j[pn+k] = x_{j+1}[n]$$

$$\omega_j^{\uparrow}(x_j)[n] = y_{j+1}[n] = (y_{j+1,1}[n], y_{j+1,2}[n], \ldots, y_{j+1,p-1}[n])$$

where $y_{j+1,r}[n] = x_j[pn+r] \oslash x_j[pn]$ with r = 1, 2, …, p – 1

While synthesis operation are constructed as follows:

$$\Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn] = x_{j+1}[n] \oslash \left[\left(\bigoplus_{k=1}^{p-1} y_{j+1,k}[n]\right) \oplus 0\right]$$

$$\Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn+r] = \Psi_j^{\downarrow}(x_{j+1}, y_{j+1})[pn] \otimes y_{j+1,r}[n]$$

with r = 1, 2, …, p – 1

2.2 Construction Of Cryptographic Algorithm

Based on the max plus wavelet transform, cryptographic algorithm will be constructed. This section presents the encryption technique, decryption technique and key generating.

2.2.1 Encryption Technique

Step 1: The message is converted into ASCII code and then it is stored in array **Plain ASCII**.
Step 2: The first element of the key is entered. It is the number of the channels used.
Step 3: The **Plain ASCII** is put into the analysis process using number of the channels correspond to the key.
The approximation signal, detail signals and the second element of the key are obtained from the analysis process. The process of key generating will explained in subsection 2.2.2.
Step 4: The approximation signal and the absolute value of the detail signals are stored in array **Cipher ASCII**.
Step 5: **Cipher ASCII** is converted into text and then it is stored in variable **Cipher text**.
Then Cipher text and the key will be sent to the receiver.

2.2.2 Key Generating

The cryptographic key consists of two elements. The first element is the number of the channels used. The second element is the code for the detail signals. The second element of the key is generated as follows:
1. The negative detail signal is given code 1, while positive is given code 0.

2. Every 8 number of the code will be transformed to a binary number, and also for the rest of the code.
3. The binary numbers are converted into integers. The integers are the second element of the key.

2.2.3 Decryption Technique

Step 1: The encrypted message (Cipher text) is converted into ASCII code and then it is stored in array **Cipher ASCII**.
Step 2: The cryptographic key is entered.
Step 3: The first element of the key is extracted to get the number of the channels used. The rest of the key is taken as the second element of the key. It is converted into binary number.
Step 4: The detail signals can be obtained using the binary number. While the approximation signal is the first number of **Cipher ASCII**.
Step 5: The approximation signal and detail signals are put into the synthesis process using the number of the channels correspond to the key.
Step 6: The main signals are obtained from the synthesis process and these are stored in array **Plain ASCII**.
Step 7: The original messages can be retrieved by transform **Plain ASCII** to their corresponding ASCII characters.

3. RESULTS AND DISCUSSION

This program works perfectly for the text format i.e. **.txt** files. For example, the first experiment with the original message "**Shabieq El-Fathin Attaraufaa'** " (the messages in bold font and be among " "). Using the first element of the key [2 3 5], be obtained ciphertext i.e. "**' (++I&!%K+& "4=5!$qG93!nS31/ '**" (the messages in bold font and be among " ") and the second element of the key i.e. [11 216 194 29]. Decryption process is done by the key i.e. [2 3 5 11 216 194 29].

One of the cryptographic algorithm criteria is the level of confusion and diffusion [6]. The level of confusion can be determined by calculate the correlation value between the plaintext and ciphertext. The correlation value in the first experiment is 0.126543374. The contrast between plaintext and ciphertext in the first experiment is given in Figure 3.

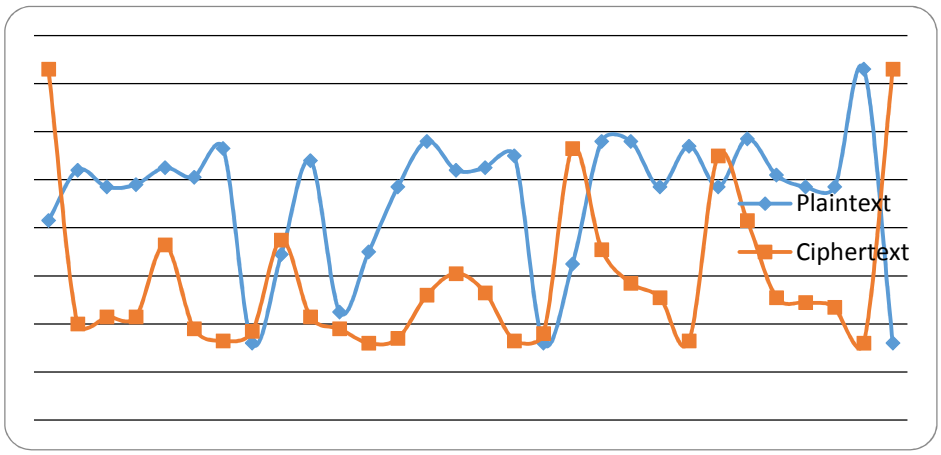

Figure 3 the Contrast between Plaintext and Cipher text

From Figure 3 we can clearly notice that for each character on the plaintext transforms to different character in the cipher text, and there is no direct relationship between the plaintext and the cipher text. These indicate that the proposed algorithm has high confusion because the relationship between the plaintext and the cipher text is nonlinear.

We observed that the message has some repeated characters such as character "a" for example (repeated five times), and every time the resulted cipher is different from the other. This indicates that the proposed algorithm provides a high level of diffusion. A comparative of the correlation value between the plaintext and cipher text for texts varying in length is shown in the Table 1. From Table 1 we observed that the correlation value decreases along with increasing length of the text.

The encryption time in the first experiment is 0.016 seconds, while decryption time is 0.015 seconds. A comparative of the encryption and decryption time for texts varying in length is shown in the Table 2. The table shows that the encryption and decryption time increases linearly along with increasing length of the text. The decryption time is seen faster than the encryption time.

Table 1 The Correlation Value between Plaintext and Cipher text

Length of Text	Correlation Value
30	0.126543374
100	0.05135685
300	0.094886202
600	0.035254875
1000	0.023059525
3000	0.016014888
6000	0.009566434
10000	0.00004862

Table 2 Encryption and Decryption Time

Length of Text	Encryption Time (Second)	Decryption Time (Second)
30	0.016	0.015
100	0.031	0.016
300	0.047	0.046
600	0.093	0.078
1000	0.172	0.125
3000	0.515	0.484
6000	1.451	1.388
10000	2.262	2.09

4. CONCLUSION

The max plus wavelet transform can be used for construct a cryptographic algorithm. This cryptographic algorithm can reconstructs the cipher text into plaintext very well. Encryption and decryption time are fast and increase linearly along with increasing length of the text. These show that the proposed algorithm is efficient in the running time. This cryptographic algorithm has small correlation value between plaintext and cipher text, this meaning almost no linear correlation between the plaintext and cipher text. Each character in the plaintext will be several different characters in the cipher text. These show that the proposed algorithm has high level of confusion and diffusion.

5. REFERENCES

1. D. Goswami, N. Rahman, J. Biswas, A. Koul, R.L. Tamang, A.K. Bhattacharjee, 2011, A Discrete Wavelet Transform based Cryptographic algorithm, *International Journal of Computer Science and Network Security*, Vol. 11, No. 4.
2. K. Fahim, 2014, Konstruksi Transformasi Wavelet Menggunakan Aljabar Max Plus, Master's Thesis in Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.
3. D. Grigoriev, V. Shpilrain, 2013, Tropical Cryptography, *International Association for Cryptologic Research*.

4. M. Durcheva, 2015, Some applications of idempotent semirings in Public Key Cryptography, *ACM Communication in Computer Algebra*, 19.
5. S. Kromodimoeljo, 2010, Teori Dan Aplikasi Kriptografi, SPK IT Consulting.
6. C. E. Shannon, 1949, Communication Theory Of Secrecy Systems, *Bell Systems Technical Journal*, Vol. 28.
7. Subiono, 2015, Aljabar Min Max Plus Dan Terapannya, Department of Mathematics, Sepuluh Nopember Institute of Technology, Surabaya.